

複製できないのに、訂正はできる

— シンドロームは誤りについて **8** ビット語り、状態については **0** ビット語る — 盗聴も同じ理屈で
25% という数になって現れる — [論文281]

山岸 勇輝 (Yuuki YAMAGISHI)

Yamagishi Complexity Torus Lab, Japan | 山岸勇輝ラボ

2026年8月

— *From thinking to syncing.* —

要旨

量子状態は複製できない（複製不可能定理）。ところが量子誤り訂正は動く。訂正するには誤りを知らねばならず、知るには測らねばならず、測れば状態は壊れる——はずである。本稿が問うのは、この二つがなぜ両立するかである——答は、測っているのが状態ではなく誤りだからである。新しい数学定理も新しい法則も主張しない。第一に、シンドロームが語るビット数を数える。ショアの **9** 量子ビット符号は誤りについて **8** ビット語り、論理状態については **0** ビット語る（第2節）。第二に、**5** 量子ビット符号ではちょうど飽和する。シンドローム数 **16** に対し、訂正すべき誤りが **16** 通り——一つも余らない（第3節）。第三に、同じ理屈が盗聴を数にする。BB84 の傍受再送で、誤り率は **25%** ちょうどになる（第4節）。第四に、**25%** は安全限界の **2.27** 倍である。片方向後処理の限界は **11.0028%** であり、確実に検出される（第5節）。第五に、**73** ビット照合すれば見逃し確率は 10^{-9} を切る。**0.75⁷³** である（第5節）。第六に、分離子は「安全性の根拠が計算量でない」ことである。計算機が速くなっても、**25%** は **25%** のままである（第6節）。

本稿の射程 (scope note) : 新しい数学定理も新しい法則も主張しない——複製不可能定理、ショアの 9 量子ビット符号、5 量子ビット符号、BB84、傍受再送攻撃の 25%、ショア=プレスキルの 11% は、いずれも標準的である。符号を作らない——数えるのはシンδροームの個数と、訂正すべき誤りの個数だけである。複製不可能定理を証明しない——引くだけである。安全性証明をしない——ショア=プレスキルの 11.0028% は数値として引くのみで、証明には立ち入らない。現実の量子鍵配送を論じない——損失、暗黒計数、多光子成分、装置攻撃を一切扱わない。本稿の 25% は理想的な傍受再送のみの値である。最良の攻撃を主張しない——傍受再送は最良の攻撃ではない。より賢い攻撃は同じ情報量をより少ない誤り率で得る。25% は「素朴な攻撃がどれだけ目立つか」の数である。有限鍵効果を扱わない——第5節の 0.75^{73} は全量傍受のときの見逃し確率であり、統計的安全性の完全な評価ではない。量子計算を論じない——ショアの因数分解も、閾値定理も扱わない。既刊との関係：論文 163 は「良い符号が在る」と「これが良い符号だ」を分けた——本稿は構成の側に立ち、具体的な符号のシンδροームを数える。論文 252 は「情報量」が四つあることを数えた——本稿が数える 8 と 0 は同じ一つの測定が、二つの対象について返すビット数であり、量の種類ではなく対象の分離である。論文 188 は未知数より少ない測定で厳密に決まる場合を扱った——本稿はその逆で、必要な分だけ測って、それ以外を測らない場合である。論文 179 は「構成できない」に別根があることを示した——複製不可能定理も一つの「構成できない」であり、本稿はその根が線型性にあることを前提として使う。論文 68 は量子ビットをホップ束として読んだ——本稿は同じ量子ビットを、情報のビット数として数える。加えたのはシンδροームが語るビット数を「誤りについて 8 / 状態について 0」と分けて数えたこと、5 量子ビット符号で $16 = 16$ とちょうど飽和することを確かめたこと、同じ理屈が BB84 の 25% を生むと並べたこと、25% が安全限界の 2.2722 倍だと計算したことである。

1. 記法と、両立しないはずの二つ

一つめ：複製不可能定理——未知の量子状態を複製する操作は存在しない。

二つめ：量子誤り訂正——符号化された状態に誤りが入っても、元に戻せる。

両立しないように見える理由：訂正するには、どの誤りが入ったかを知らねばならない。知るには測らねばならない。量子状態を測れば、状態は壊れる。

答：測っているのは状態ではない。測っているのは誤りの種類である。

本稿の方法：この区別を、ビット数を数えることで示す。

2. シンδροームが語るビット数を数える

設定： n 個の物理量子ビットに k 個の論理量子ビットを埋め込む。安定符号では、生成元の個数は $n - k$ 個であり、それぞれが ± 1 を返す。

検算 2.1：ショアの 9 量子ビット符号 ($n = 9$, $k = 1$)。

量	値
物理量子ビット n	9
論理量子ビット k	1
生成元の個数 $n - k$	8
シンドローームの場合の数 2^8	256
訂正すべき 1 量子ビット誤り $1 + 3n$	28
余り	228

観察 2.2

シンドローームは 8 ビットを返す。その 8 ビットはどこにどの誤りが入ったかを語る。

観察 2.3

これが本稿の芯である。その 8 ビットが論理状態について語るビット数は 0 である。生成元は論理演算子と可換なので、測っても論理状態の重ね合わせを壊さない——複製していないし、覗いてもいない。

検算 2.4：三つの符号で同じ数え方をする。

符号	n	生成元	シンドローーム数	訂正すべき誤り	状態について
ショア	9	8	256	28	0 ビット
ステイン	7	6	64	22	0 ビット
5 量子ビット	5	4	16	16	0 ビット

観察 2.5

右端の列がどれも 0 である。符号が大きくなっても、シンドローームが状態について語る量は増えない——これが両立の理由である。

3.5 量子ビット符号は、ちょうど飽和する

設定：シンドローームで誤りを見分けるには、シンドローーム数 $\geq$ 訂正すべき誤りの数が必要。 $k = 1$ 、距離 3 なら $1 + 3n \leq 2^{n-1}$ である（量子ハミング限界）。

検算 3.1：

n	$1 + 3n$	2^{n-1}	可否
3	10	4	不可
4	13	8	不可
5	16	16	ちょうど
6	19	32	余る
7	22	64	余る
9	28	256	余る

観察 3.2

$n = 5$ で等号が成り立つ。16 個のシンドローームが 16 通りの誤りにちょうど一対一で対応し、一つも余らない——完全符号である。

観察 3.3

$n = 4$ は $13 > 8$ で不可である。1 量子ビットの誤りを訂正するには、最低 5 個要る——ここに正確な下限がある。

観察 3.4

論文179 は「構成できない」にも別根があると言った。 $n = 4$ が構成できない根は数え上げである—— $1 + 3n \leq 2^{n-1}$ という不等式を解くだけで $n \geq 5$ が出る。量子力学の詳細は要らない。

4. 同じ理屈が、盗聴を数にする

設定：BB84。アリスは二つの基底（直線・斜め）のどちらかを乱数で選び、ビットを送る。ボブも乱数で基底を選ぶ。エヴは途中で測り、測った結果を送り直す（傍受再送）。

検算 4.1：ボブの基底がアリスと一致した場合だけを見る（篩い分け後）。

エヴの基底	確率	再送される状態	ボブの誤り率
アリスと一致	1/2	正しい	0
アリスと不一致	1/2	45° ずれ	1/2
合計			$\frac{1}{2} \cdot 0 + \frac{1}{2} \cdot \frac{1}{2} = 0.25$

観察 4.2

誤り率は **25%** ちょうどである。エヴは測ったから目立つ——第2節のシンドロームが測っても目立たないのと、ちょうど裏表である。

検算 4.3：エヴがどれだけ得たかを数える。

量	値
エヴのビットが当たる確率	$\frac{1}{2} \cdot 1 + \frac{1}{2} \cdot \frac{1}{2} = 0.75$
相互情報量 $1 - h(1/4)$	0.188722 ビット

観察 4.4

エヴは 1 ビットあたり **0.19** ビットしか得ないのに、**25%** の誤りを残す。取り分に対して、足跡が大きすぎる。

観察 4.5

正直に書くべき点——傍受再送は最良の攻撃ではない。より賢い攻撃は、同じ情報をより少ない誤りで得る——**25%** は「素朴な攻撃がどれだけ目立つか」の数であって、安全性の証明ではない。

5. 25% は、限界の 2.27 倍である

設定：誤り率 q から鍵を取り出せるかは、片方向後処理では $R = 1 - 2h(q)$ で決まる（ショア＝プレスキル）。

検算 5.1：

誤り率 q	$h(q)$	鍵率 $R = 1 - 2h(q)$
0	0	+1.000000
0.01	0.080793	+0.838414
0.02	0.141441	+0.717119
0.05	0.286397	+0.427206
0.08	0.402179	+0.195642
0.110028	0.500000	0
0.15	0.609840	-0.219681
0.25	0.811278	-0.622556

観察 5.2

限界は **11.0028%** である。傍受再送の **25%** はその **2.2722** 倍——境界のすぐ外ではなく、はるかに外側にある。

検算 5.3：一部だけ傍受すれば隠れられるかを見る。割合 f だけ傍受すると誤り率は $0.25f$ である。

量	値
$0.25f \leq 0.110028$ となる f の上限	0.440111
そのときエヴが得る情報	0.083059 ビット/節いビット

観察 5.4

隠れることはできる。ただし取り分は **1** ビットあたり **0.083** ビットに落ちる——隠れるほど、取れなくなる。

検算 5.5：全量傍受のとき、 n ビット照合して一つも誤りが出ない確率は 0.75^n である。

n	0.75^n
10	5.63×10^{-2}
20	3.17×10^{-3}
50	5.66×10^{-7}
73	7.58×10^{-10}
100	3.21×10^{-13}
200	1.03×10^{-25}

観察 5.6

73 ビット照合すれば、見逃し確率は 10^{-9} を切る。鍵が何万ビットあろうと、確かめるのに要るのは **73** ビットである。

6. 分離子：安全性の根拠が、計算量ではない

観察 6.1

分離子——何を動かすと、この **25%** は別の数になるか。測定理論を変えるしかない。

観察 6.2

計算機を速くしても 25% は動かない。鍵を長くしても動かない。アルゴリズムを賢くしても動かない——25% は基底の重なりから出る数であって、計算量から出る数ではない。

観察 6.3

これは古典暗号と身分が違う。古典暗号の安全性は「解くのが難しい」であり、難しさは計算機の速さに対する相対量である。ここでの安全性は「測れば目立つ」であり、相手の計算力に依存しない。

観察 6.4

第2節と第4節は、同じ一つの事実の裏表である。

	誤りについて	状態について
シンδροーム測定（第2節）	8 ビット得る	0 ビット得る $\Rightarrow$ 壊さない
エヴの測定（第4節）	—	得ようとする $\Rightarrow$ 壊す（25%）

観察 6.5

したがって「複製できないのに訂正できる」は矛盾ではない。複製も観測もしていない——状態について 0 ビットしか取っていないから、代償も 0 である。

7. 点呼と結び

1. ショア符号のシンδροームは 8 ビット（検算2.1）： $2^8 = 256$ 通り。
2. そのうち状態について 0 ビット（観察2.3）：だから壊れない。
3. 三つの符号すべてで 0（検算2.4）：大きくしても増えない。
4. 5 量子ビットで $16 = 16$ （検算3.1）：ちょうど飽和する。
5. $n = 4$ は $13 > 8$ で不可（観察3.3）：最低 5 個要る。
6. 傍受再送の誤り率 25%（検算4.1）： $\frac{1}{2} \cdot \frac{1}{2}$ 。

7. エヴの取り分 **0.188722** ビット (検算4.3) : 足跡に対して小さい。
8. 安全限界 **11.0028%** (検算5.1) : **25%** はその **2.2722** 倍。
9. 隠れると **0.083059** ビット (検算5.3) : 隠れるほど取れない。
10. **73** ビットで 10^{-9} (検算5.5) : 確かめるのは短くて済む。

結び : 複製できないのに訂正できるのは、測っているのが状態ではないからである。ショアの **9** 量子ビット符号のシンδροームは、誤りについて **8** ビットを語り、論理状態については **0** ビットを語る——**0** ビットしか取らないから、代償も **0** である。符号を大きくしてもこの **0** は増えない——ショアもステインも **5** 量子ビット符号も、状態については等しく **0** である。そして **5** 量子ビット符号では、**16** 個のシンδροームが **16** 通りの誤りにちょうど一対一で対応する。同じ理屈の裏側が、盗聴を数にする——エヴは状態について取ろうとするので、**25%** という足跡が残る。それは安全限界 **11.0028%** の **2.2722** 倍であり、**73** ビット照合すれば見逃し確率は 10^{-9} を切る。分けるものは一つ——その測定が、状態について何ビット取っているかを数えること。数えれば、訂正と盗聴が同じ一つの原理の裏表だと分かる。数えなければ、両者は矛盾して見える。

参考文献

1. Wootters, W. K. and Zurek, W. H. (1982). A Single Quantum Cannot Be Cloned. *Nature*, 299(5886).
2. Shor, P. W. (1995). Scheme for Reducing Decoherence in Quantum Computer Memory. *Physical Review A*, 52(4).
3. Steane, A. M. (1996). Error Correcting Codes in Quantum Theory. *Physical Review Letters*, 77(5).
4. Laflamme, R., Miquel, C., Paz, J. P. and Zurek, W. H. (1996). Perfect Quantum Error Correcting Code. *Physical Review Letters*, 77(1).
5. Bennett, C. H. and Brassard, G. (1984). Quantum Cryptography: Public Key Distribution and Coin Tossing. In *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*.
6. Shor, P. W. and Preskill, J. (2000). Simple Proof of Security of the BB84 Quantum Key Distribution Protocol. *Physical Review Letters*, 85(2).
7. Nielsen, M. A. and Chuang, I. L. (2010). *Quantum Computation and Quantum Information*. Cambridge: Cambridge University Press.
8. Gottesman, D. (1997). *Stabilizer Codes and Quantum Error Correction*. PhD thesis, California Institute of Technology.
9. 山岸勇輝 (2026). *Hopf束としての量子ビット — ボルン則の「2」とHopf写像の「2」は同根か韻か* [論文68]. Zenodo. 10.5281/zenodo.21642238
10. 山岸勇輝 (2026). 「良い符号が在る」と「これが良い符号だ」は、別の文である [論文163]. Zenodo. 10.5281/zenodo.22092677
11. 山岸勇輝 (2026). 「構成できない」にも別根がある [論文179]. Zenodo. 10.5281/zenodo.22098419
12. 山岸勇輝 (2026). 未知数より少ない測定で、厳密に決まる [論文188]. Zenodo. 10.5281/zenodo.22105691
13. 山岸勇輝 (2026). 「情報量」は四つあり、要るものが違う [論文252]. Zenodo. 10.5281/zenodo.22161148

— *From thinking to syncing.* —

山岸 勇輝 (Yuuki YAMAGISHI)

© 2026 Yamagishi Complexity Torus Lab, Japan · Licensed under Creative Commons Attribution 4.0 International (CC BY 4.0)